



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/796,972	03/11/2004	Masaya Yamamoto	2004_0392A	4039
513 7590 10/14/2009 WENDEROTH, LIND & PONACK, L.L.P. 1030 15th Street, N.W., Suite 400 East Washington, DC 20005-1503				
EXAMINER KANAAN, SIMON P				
ART UNIT		PAPER NUMBER		
2432				
MAIL DATE		DELIVERY MODE		
10/14/2009		PAPER		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

### Office Action Summary

**Application No.**

10/796,972

**Applicant(s)**

YAMAMOTO ET AL.

**Examiner**

SIMON KANAAN

**Art Unit**

2432

**Period for Reply** -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 09 September 2009.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 19-22, 24-31 and 33-42 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 19-22, 24-31 and 33-41 is/are rejected.
- 7) ☐ Claim(s) 42 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

**DETAILED ACTION**

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 9/9/2009 has been entered.

***Applicant's Arguments***

2. Applicant argues that the cited prior art does not disclose:
- a. "cryptographically calculating a medium content key using the medium information and the information pre-stored in the playback terminal itself;"
  - b. "cryptographically calculating a license content key using the medium content key and the managed information acquired from the external license server;"

***Examiner's Response to Arguments***

3. Applicant's arguments, see Amendments and Remarks, filed January 26, 2009, with respect to the rejection(s) of claim(s) 19-22, 24-32 and 33-41 have been fully considered and are not persuasive
- a. "cryptographically calculating a medium content key using the medium information and the information pre-stored in the playback terminal itself;" - BluRay and CSS discs teach the encrypted content is being generated by encrypting content using a medium content key, which is based on the medium information and the play back

device, and using also information pre-stored in the playback terminal, so that encrypted content is decrypted by use of the information pre-stored in the playback terminal itself [Specification Admitted Prior Art: Page 2: 14-21].

b. “cryptographically calculating a license content key using the medium content key and the managed information acquired from the external license server;” [Oshima 6: 47-67, password is from other keys, i.e. key generated from key].

*Allowable Subject Matter*

2. Claim 42 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

*Claim Rejections - 35 USC § 112*

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 19-22, 24-32 and 33-41 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The newly added limitations: “cryptographically calculating a medium content key using the medium information and the information pre-stored in the playback

terminal itself;” and “cryptographically calculating a license content key using the medium content key and the managed information acquired from the external license server;” can not be found in the originally filed specification. In the originally filed specification a license is obtained that includes a decryption key and a content key is obtained from the license.

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 19-22, 24-32 and 33-41 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. They recite the terms “medium content key” and “license content key” both of which are not in the specification and there is no clear definition in the claim.

#### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 19-22, 24-32 and 33-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sims III [US 2002/0016919 A1], and further in view of Admitted Prior Art [Specification Prior Art Section], and Oshima [US 7191154 B2].

As per claim 28, Sims III discloses a content playback method used in a playback terminal for playing back content, the content playback method comprising:

reading encrypted content from a portable medium [Sims III 9: 0097 --Encrypted disk key is provided to the play-back device decoder to allow meaningful use of the content recorded thereon.],

the encrypted content being generated by encrypting content using at least medium information pre-recorded on the portable medium [Sims III 6: 0057 --For example, (Disk Key) in some cases it may be used to encrypt/decrypt content.];

judging whether or not information managed by an external license server is required for decrypting the encrypted content [Sims III 9: 0098];

reading the medium information pre-recorded on the portable medium [Sims III 8: 0091];

acquiring the managed information managed by the external license server when it is judged that the managed information is required [Sims III 9: 0098],

the managed information managed by the external license server being part of information which is required for the decryption of the encrypted content [Sims III 9: 0098 -- Managed information is associated with rights/authorization of acquiring a cryptographic key necessary in utilizing the content of media.];

and a decryption step of (a) decrypting the encrypted content using the medium content key, when it is judged that the managed information is not required, [Sims III 8: 0091] [Sims III 9: 0097]

and (b) decrypting the encrypted content using the licensed content key when it is judged that the information is required [Sims III 10: 0106].

But, Sims III does not teach the encrypted content is being generated by encrypting content using also information pre-stored in the playback terminal. And cryptographically calculating a medium content key using the medium information and the information pre-stored in the playback terminal itself; cryptographically calculating a license content key using the medium content key and the managed information acquired from the external license server;

However, BlueRay and CSS discs teach the encrypted content is being generated by encrypting content using a medium content key, which is based on the medium information and the play back device, and using also information pre-stored in the playback terminal, so that encrypted content is decrypted by use of the information pre-stored in the playback terminal itself [Specification Admitted Prior Art: Page 2: 14-21] and downloading a license from a server [Specification Admitted Prior Art: Page 2 line 22- page 3 line 4].

It would have been obvious to one of ordinary skilled in the art at the time of invention to modify Sims III by also using information pre-stored in the playback terminal when generating encrypted content, so that encrypted content is decrypted by use of the information pre-stored in the playback terminal itself as taught by the admitted prior art. The suggestion/motivation would have been to have encrypted content stored in the medium be tied to a particular playback terminal holding the pre-stored information, since the encrypted content cannot be decrypted with stolen medium information in the absence of the pre-stored information, thus increasing security.

Sims III, in view of the admitted prior art does not teach that when it is judged that the managed information is required, decrypting the encrypted content using the managed information acquired from the external license server, and also the medium information. cryptographically calculating a license content key using the medium content key and the managed information acquired from the external license server;

Oshima teaches that when managed information is required to decrypt encrypted content, the encrypted content is decrypted using the managed information acquired from an external license server [Oshima 6: 42-49], and also medium information [Oshima 6: 58-67].

cryptographically calculating a license content key using the medium content key and the managed information acquired from the external license server; [Oshima 6: 47-67, password is from other keys, i.e. key generated form key].

It would have been obvious to one of ordinary skilled in the art at the time of invention to modify Sims III in view of the admitted prior art by decrypting encrypted content using the managed information and also medium information, when managed information is required as taught by Oshima. The suggestion/motivation would have been to prevent decryption of encrypted content using other mediums with stolen acquired managed information, and vice versa, thus increasing security.

As per claim 41, Sims teaches the content playback method of claim 28, wherein the managed information managed by the external license server is rights information including usage rights for the content [Sims III 9: 0100 –rights information is associated with determination of single use or unlimited use by external source.],



the judging comprises judging whether or not the rights information is required, as the information managed by the external license server, for decrypting the encrypted content [Sims III 9: 0098],

the acquiring comprises acquiring the rights information from the external license server when it is judged that the rights information is required [Sims III 9: 100-101 --acquiring the requested information associated with single use or unlimited use],

and the decryption step comprises (a) decrypting the encrypted content using the medium content key when it is judged that the rights information is not required [Sims III 8: 0091] [Sims III 9: 0097],

and (b) decrypting the encrypted content using the license content key, when it is judged that the rights information is required [Sims III 10: 0106].

But Sims III does not teach the encrypted content is being generated by encrypting content using also information pre-stored in the playback terminal, so that encrypted content is decrypted by use of the information pre-stored in the playback terminal itself.

BlueRay and CSS discs teach the encrypted content is being generated by encrypting content using also information pre-stored in the playback terminal, so that encrypted content is decrypted by use of the information pre-stored in the playback terminal itself [Specification Admitted Prior Art: Page 2: 14-21].

It would have been obvious to one of ordinary skilled in the art at the time of invention to modify Sims III by also using information pre-stored in the playback terminal when generating encrypted content, so that encrypted content is decrypted by use of the information pre-stored in the playback terminal itself as taught by the admitted prior art. The suggestion/motivation would

have been to have encrypted content stored in the medium be tied to a particular playback terminal holding the pre-stored information, since the encrypted content cannot be decrypted with stolen medium information in the absence of the pre-stored information, thus increasing security.

Sims III, in view of the admitted prior art does not teach that when it is judged that the rights information is required, decrypting the encrypted content using the rights information, and also the medium information.

Oshima teaches managed information managed by the external license server is rights information including usage rights for the content [Oshima 6: 47-48 --...time data representing the period of use allowed.],

the judging comprises judging whether or not the rights information is required, as the information managed by the external license server, for decrypting the encrypted content [Oshima 5: 12-17 --In order to get a password, the connection address...which is the server of a password issue center...is accessed.],

the acquiring comprises acquiring the rights information from the external license server when it is judged that the rights information is required [Oshima 6: 46-49],

and the decryption step comprises decrypting the encrypted content using the rights information [Oshima 6: 42-49],

and medium information [Oshima 6: 58-67],

when it is judged that the rights information is required [Oshima 5: 13 --In order to get a password...].

It would have been obvious to one of ordinary skilled in the art at the time of invention to modify Sims III in view of the admitted prior art by decrypting encrypted content using the managed information and also medium information, when managed information is required as taught by Oshima. The suggestion/motivation would have been to prevent decryption of encrypted content using other mediums with stolen acquired managed information, and vice versa, thus increasing security.

As per claim 29, Sims III, in view of the admitted prior art, and Oshima teaches the content playback method of claim 41, wherein the medium information includes a media key [Sims III 7: 0071 --Disk Key],

The cryptographically calculating of the medium content key comprises cryptographically calculating the medium content key using the media key of the medium information, - BlueRay and CSS discs teach the encrypted content is being generated by encrypting content using a medium content key, which is based on the medium information and the play back device, and using also information pre-stored in the playback terminal, so that encrypted content is decrypted by use of the information pre-stored in the playback terminal itself [Specification Admitted Prior Art: Page 2: 14-21]

and the decryption step includes: a content key obtaining sub-step of, when it is judged that the rights information is not required, obtaining the medium content key used in decrypting of the encrypted content [Sims III 9: 0097 --Use Disk key as Content key];

and a content decryption sub-step of, when it is judged that the rights information is not required, decrypting the encrypted content using the medium content key [Sims 6: 0057].

As per claim 30, Sims III, in view of admitted prior art and Oshima teaches the content playback method claim 29, wherein the content key obtaining sub-step includes, when it is judged that the rights information is required, obtaining the license content key used in decrypting of the encrypted content [Oshima 6: 65 --The '1-nth' decoding key is output to the cipher decoder.],

and the content decryption sub-step includes, when it is judged that the rights information is required, decrypting the encrypted content using the license content key [Oshima 6: 66-67].

As per claim 31, Sims III, in view of admitted prior art and Oshima teaches the content playback method of claim 30, wherein the rights information includes a rights key [Oshima 5: 13 --password],

The cryptographically calculating of the license content key comprises cryptographically calculating the license content key using the rights key of the rights information, [Oshima 6: 47-67, password is from other keys, i.e. key generated from key].

and the content key obtaining sub-step includes, when it is judged that the rights information is required, obtaining the license content key using the rights key [Oshima 6: 55-66].

As per claim 33, Sims III, in view of the admitted prior art and Oshima teaches the content playback method of claim 30, wherein the portable medium further has stored thereon

key obtaining information indicating whether or not the rights information is required for obtaining a key used for decrypting the encrypted content [Sims 8: 0086-0088],

and the content playback method further comprises: reading the key obtaining information from the portable medium [Sims 8: 0091] [Sims 9: 0102],

wherein the judging comprises judging whether or not the rights information is required for decrypting the encrypted content, based on the key obtaining information [Sims 9: 0098].

As per claim 34, Sims III in view of the admitted prior art and Oshima teaches the content playback method of claim 29, wherein the decryption step includes, when it is judged that the rights information is necessary, performing decryption of the encrypted content only when the acquiring has already acquired the rights information [Oshima 6: 58]

and the rights information indicates that usage of the content is permitted [Oshima 6: 62-63 --timing data is checked for validity].

As per claim 35, Sims III, in view of the admitted prior art and Oshima teaches the content playback method of claim 29, wherein the playback terminal includes a holding unit operable to hold device unique information that is unique to the playback terminal [Sims 4: 0036-0037],

the media key is in an encrypted state [Sims 9: 0097 --encrypted Disk Key],

having been encrypted using the device unique information [Sims 9: 0097 --encrypted with the public key of the matching "acceptable user"]],

and the cryptographically calculating of the medium content key includes, when it is judged that the rights information is not required, obtaining the media key by decrypting the encrypted-state media key using the device unique information [Sims 9: 0097 --decrypted with the private key of the matching "acceptable user."].

As per claim 36, Sims III, in view of the admitted prior art and Oshima teaches the content playback method of claim 29, wherein the portable medium further has stored thereon information indicating whether or not the rights information is required for decrypting of the encrypted content [Sims 8: 0086-0088],

and the content playback method further comprises: reading the information from the portable medium [Sims 8: 0091] [Sims 9: 0102],

wherein the judging comprises judging whether or not the rights information is required for decrypting the encrypted content, based on the information [Sims 9: 0098].

Claims 19-22 and 24-27 are rejected because it is similar matter to claims 28—31 and 33-36.

Claim 37 is rejected because it is the portable recording medium comprising the same elements as claim 19.

Claim 38 is rejected because it is similar matter to claim 41.

As per claim 39, Sims III, in view of admitted prior art and Oshima teaches the playback terminal of claim 20, wherein the rights information includes information showing permission to play back the content [Oshima 6: 62-63 --timing data representing the period of use allowed.].

As per claim 40, Sims III teaches the playback terminal of claim 39, wherein the portable medium further has recorded thereon information indicating whether or not the rights information is necessary for decrypting the encrypted content [Sims 6: 0057-0066],

and the decryption method judgment unit judges whether or not the rights information is required for decrypting the encrypted content based on the information recorded on the portable medium [Sims 8: 0091; 9: 0098; 9: 0102].

### **Conclusion**

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Simon Kanaan whose telephone number is (571) 270-3906. The examiner can normally be reached on Monday to Friday 8:30 AM to 5:00 PM. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

If attempts to reach the above noted Examiner by telephone are unsuccessful, the Examiner's supervisor, Gilberto Barron, can be reached at the following telephone number: (571) 272-3799.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/SIMON KANAAN/  
Examiner, Art Unit 2432

/Gilberto Barron Jr./  
Supervisory Patent Examiner, Art Unit 2432